S05P0372WO00

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04L 9/18, G07F 7/10 — A1

(11) Internationale Veröffentlichungsnummer: **WO 98/48540**

(43) Internationales Veröffentlichungsdatum: 29. Oktober 1998 (29.10.98)

(21) Internationales Aktenzeichen: PCT/EP98/01391

(22) Internationales Anmeldedatum: 11. März 1998 (11.03.98)

(30) Prioritätsdaten:
197 16 861.2 22. April 1997 (22.04.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich–Ebert–Allee 140, D–53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: KOWALSKI, Bernd [DE/DE]; Am Bastenberg 4, D–57072 Siegen (DE). WOLFENSTETTER, Klaus–Dieter [DE/DE]; Neckarstrasse 19, D–64673 Zwingenberg–Rodau (DE).

(81) Bestimmungsstaaten: CA, CN, JP, KR, TR, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

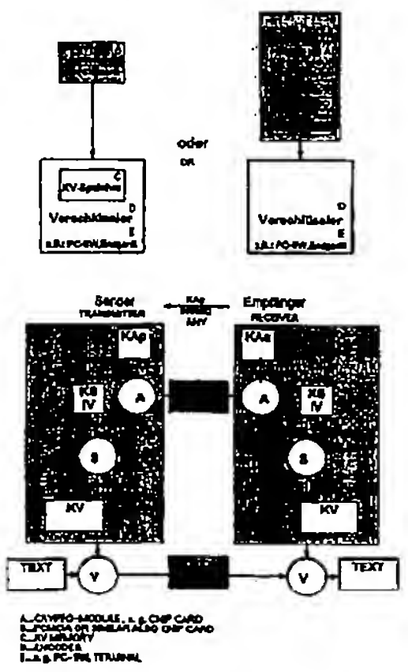
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: ENCRYPTION METHOD AND DEVICE

(54) Bezeichnung: VERSCHLÜSSELUNGSVERFAHREN UND –VORRICHTUNG

(57) Abstract

The invention relates to an economical method and device for implementing even high–performance encryption functions in an encoder consisting of only a PC, software device or similar or any preferred terminal or information system, with an integrated Vernam cipher which does not need to be supported by expensive crypto–hardware for the necessary encryption process. The crypto–hardware consists of either a chip card or a multi–functional PC interface adapter (PCMCIA module) with built–in special crypto–hardware. The encryptor is simply a conventional PC, a software device or another terminal which requires no crypto–technology other than the very simple Vernam cipher (for example, EXOR), even for wideband applications in software. The external crypto–modules all contain complex crypto–functions which produce the Vernam key in reserve. These reserves are temporarily stored in an intermediate memory and then used up progressively by the encryption process through logical operations. Said memory can be installed in either the PC/terminal or in the crypto–module. The encoder always operates with the same Vernam cipher, even if the external crypto– or PCMCIA modules use different symmetrical and asymmetrical ciphers. External crypto–modules in the form of chip cards or PCMCIA modules are economical to produce. All of the complex crypto–functions are outside of the encryptor. They can be interchanged by module and can be performed in the inexpensive and somewhat slower crypto–modules suggested by the invention.



(57) Zusammenfassung

Es wird ein Verfahren und eine Vorrichtung zur kostengünstigen Implementierung auch von hochperformanten Verschlüsselungsfunktionen in einem Verschlüssler vorgeschlagen, der lediglich aus einer PC Software oder dergleichen oder einem beliebigen anderen Endgerät, Informationssystem mit integrierter Vernam Chiffre besteht, die für den eigentlichen Verschlüsselungsprozeß nicht durch eine aufwendige Kryptohardware unterstützt werden muß. Die Kryptohardware besteht entweder aus einer Chipkarte oder einem multifunktionalen PC Interface Adapter (PCMCIA Modul) mit eingebauter spezieller Kryptohardware. Der Verschlüssler ist hingegen ein herkömmlicher Personalcomputer (PC), Software oder ein anderes Endgerät, der jedoch außer der sehr einfachen Vernam Chiffre (zum Beispiel EXOR) auch für breitbandige Anwendungen in Software, keine weitere Kryptotechnik benötigt. Die externen Kryptomodule enthalten alle komplexen Kryptofunktionen, den Vernam–Schlüssel (KV) erzeugen sie auf Vorrat, der in einem Zwischenspeicher zwischengespeichert wird, bis er vom Verschlüsselungsprozeß durch logische Operationen des Verfahrens nach und nach verbraucht wird. Dabei kann der Speicher entweder im PC bzw. im Endgerät oder auch im Kryptomodul eingebaut sein. Der Verschlüssler arbeitet immer mit der gleichen Vernam Chiffre, auch wenn die externen Krypto– bzw. PCMCIA–Module unterschiedliche symmetrische und asymmetrische Chiffre verwenden. Externe Kryptomodule in Form von Chipkarten oder PCMCIA Modulen sind kostengünstig herzustellen. Alle komplexen Kryptofunktionen liegen außerhalb des Verschlüsslers. Sie sind modular austauschbar und lassen sich in den vorgeschlagenen preiswerten und etwas langsameren externen Kryptomodulen realisieren.

B E S C H R E I B U N G

VERSCHLÜSSELUNGSVERFAHREN UND -VORRICHTUNG

Die Erfindung betrifft ein Verfahren zur Verschlüsselung und eine Vorrichtung zur Durchführung des Verfahrens nach dem Oberbegriff des Patentanspruchs 1 bzw. des Patentanspruchs 5.

Moderne Verschlüsselungsverfahren finden zunehmende Verbreitung in der Informationsverarbeitung und Telekommunikationstechnik. Der Einsatz von Verschlüsselungsverfahren und entsprechenden Vorrichtungen wird jedoch aufgrund der nachfolgend geschilderten Probleme und Einflüsse nachhaltig behindert, obwohl durch die massenhafte Verbreitung gerade auf dem Multimediagebiet und auf dem Gebiet der Informationsverarbeitung ein sehr hoher Sicherheitsstandard gefordert wird:

- Die Verschlüsselung breitbandiger Signale erfordert den Einbau kostspieliger Kryptohardware in Personalcomputer und Endgeräte. Verfügbare preisgünstige Krypto-Chipkarten arbeiten zur Zeit nur mit einer niedrigen Durchsatzrate von deutlich unter 100 kbit/s.

- Verschlüsselungsverfahren sind häufig geschützt und nicht international standardisiert, so daß keine kostengünstigen Massenprodukte mit integrierter Kryptohardware verfügbar sind.

- Kryptohardware für breitbandige Verschlüsselung verwendet aus Kostengründen häufig nur ein einziges Verschlüsselungsverfahren. Somit können auch die damit ausgestatteten Personalcomputer und andere Endgeräte nicht eine beliebige Anzahl von Verschlüsselungs-

verfahren unterstützen. Dies führt zu einer starken Einschränkung der Kompatibilität der genannten Geräte.

- Kryptohardware unterliegt strengen internationalen Handelsrestriktionen, so daß der Export zum Beispiel von Verschlüsselungs-Endgeräten sehr stark eingeschränkt ist, weshalb die Verwendung solcher Geräte sehr stark beschränkt ist und die Preise für diese Geräte sehr hoch liegen.

In dem Buch von Alfred Beutelspacher, Kryptologie, Vieweg Verlag, 1993, sind Verschlüsselungsverfahen, wie zum Beispiel die Vernam Chiffre beschrieben und dargestellt. Außerdem sind in den ITU/CCITT Empfehlungen X.509, bzw. CACM Communications of the ACM, Vol. 21, No. 2, pp. 120-126, 1978, Verschlüsselungsverfahren wie das RSA-Verfahren beschrieben.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung zum Verschlüsseln zu schaffen, wodurch eine vereinfachte Implementierung unter Vermeidung von teurer und inkompatibler breitbandiger Verschlüsselungshardware realisierbar werden soll, so daß kostenkünstige Massenprodukte mit integrierter Kryptohardware in Zukunft ausgestattet werden können, wodurch der Sicherheitsstandard dieser Produkte wesentlich verbessert werden wird.

Die erfindungsgemäße Lösung für das Verfahren ist im Kennzeichen des Patentanspruchs 1 charakterisiert.

Weitere Lösungen bzw. Ausgestaltungen des erfindungsgemäßen Verfahrens sind in den Kennzeichen der Patentansprüche 2 bis 4 offenbart.

Die Lösung für die Implementierung der Verschlüsselungsverfahren bzw. der Vorrichtung ist in dem Kennzeichen des Patentanspruchs 5 charakterisiert. Weitere Ausgestaltungen der Vorrichtung sind in den Kennzeichen der Patentansprüche 6 und 7 charakterisiert.

Der große Vorteil der erfindungsgemäßen Lösung besteht darin, daß die Verschlüssler immer mit der gleichen Vernam Chiffre (zum Beispiel EXOR) arbeiten können. Sie sind auch dann ohne Probleme einsetzbar, wenn die externen Krypto- bzw. PCMCIA-Module (Multifunktionaler PC Interface Adapter) unterschiedliche symmetrische und asymmetrische Chiffre verwenden. Die Vernam Chiffre ist auch für hohe Durchsatzraten in Software realisierbar, so daß alle Verschlüssler ohne aufwendige Kryptohardware auskommen und in Massenprodukten kostengünstig eingesetzt werden können, da ihre Herstellung technisch einfach ist. Die externen Kryptomodule bleiben ebenfalls kostengünstig, da der auf Vorrat produzierte Vernamschlüssel auch von einer niedrig-performanten bzw. langsamen Chipkarte, zum Beispiel auf Vorrat für den Vernam-Schlüsselspeicher erzeugt werden kann, ohne den davon entkoppelt arbeitenden eigentlichen breitbandigen Verschlüsselungsprozeß zu verlangsamen.

Die Verschlüssler werden aufgrund des beschriebenen Verfahrens von den Problemen teurer, hochleistungsfähiger und untereinander inkompatibler Kryptohardware befreit. Die Vernam Chiffre ist dagegen sehr einfach und kostengünstig in Software und damit durch Speicherung zu implementieren. Alle komplexen Kryptofunktionen liegen außerhalb des Verschlüsslers. Sie sind modular austauschbar und lassen sich in den vorgeschlagenen, preiswerten und langsamen externen Kryptomodulen, zum Beispiel der Chipkarte oder der PCMCIA-Karte, realisieren. Die verwendeten Verfahren werden bei der Abstimmung zwischen Sender und Empfänger zum Beispiel auf dem Übermittlungswege ausgehandelt bzw.

"signalisiert". Der Verschlüssler selbst besteht lediglich aus einer Software, zum Beispiel PC Software oder einem beliebigen anderen Endgerät/Informationssystem mit integrierter Vernam Chiffre, die für den eigentlichen Verschlüsselungsprozeß nicht durch eine aufwendige Kryptohardware unterstützt werden muß.

Die Erfindung wird im folgenden anhand von in der Zeichnung prinzipiell dargestellten Ausführungsbeispielen näher beschrieben.

In der Zeichnung bedeuten:

Fig. 1 eine vereinfacht dargestellte bekannte Vernam Chiffre;

Fig. 2 einen modernen bekannten symmetrischen Chiffre;

Fig. 3 eine Konfiguration mit zusätzlichem Einsatz einer asymmentrischen Chiffre;

Fig. 4 eine Konfiguration mit Vernam Chiffre;

Fig. 5 eine weitere Version mit Vernam Chiffre;

Fig. 6 eine Konfiguration mit externem Kryptomodul und

Fig. 7 eine weitere Konfiguration mit Kryptomodul.

In der Zeichnung, in der nachfolgenden Beschreibung, in den Patentansprüchen und in der Zusammenfassung werden die in der hinten angegebenen Liste verwendeten Bezugszeichen bzw. Abkürzungen verwendet.

In Fig. 1 ist vereinfacht ein Vernam Chiffre dargestellt. Der hier mit "V" bezeichnete Verschlüsselungsprozeß kann

eine sehr einfache mathematische Operation, zum Beispiel EXOR sein, mit dem eine breitbandige Verschlüsselung auch in Software, das heißt ohne die Unterstützung einer speziellen Kryptohardware, möglich ist. Der Nachteil dieser bekannten Verfahren besteht jedoch darin, daß die mit "TEXT" gekennzeichnete Nachricht mit einem Vernam-Schlüssel KV verschlüsselt werden muß, der aus einer Zufallszahl mit der Länge der zu verschlüsselnden Nachricht besteht. Bei langen Nachrichten werden demnach auch lange Vernam-Schlüssel benötigt. Dadurch ist die Vernam Chiffre für den praktischen Einsatz nur bedingt verwendbar. In Fig. 2 ist ein moderner symmetrischer Chiffre S, zum Beispiel DES oder IDEA dargestellt, die auch bei relativ kurzen Schlüssellängen, üblicherweise 128 Bit für den geheimen symmetrischen Schlüssel KS, noch eine hervorragende Sicherheit bieten. DES bzw. IDEA sind Data Encryption Standards (ANSI bzw. ASCOM), ISO 9979. Allerdings muß auch hier wie bei der Vernam Chiffre der zur Ver- und Entschlüsselung erforderliche geheime Schlüssel KS über einen vom Übermittlungsweg der Nachricht unabhängigen und sicheren Kanal, zum Beispiel mittels eines Kuriers, ausgetauscht werden. Die in Fig. 3 gezeigte Konfiguration, die in der in der Einleitung angegebenen Literaturstelle näher beschrieben ist, hat den Nachteil durch den zusätzlichen Einsatz einer asymmetrischen Chiffre A, nämlich zum Beispiel dem RSA-Verfahren, zur Übermittlung des geheimen Verschlüsselungsschlüssel KS vermieden. Hierbei wird der Verschlüsselungsschlüssel KS mit dem öffentlichen asymmetrischen Schlüssel des Empfängers KAp verschlüsselt und kann von diesem anschließend mit dessen geheimen symmetrischen Schlüssel wieder entschlüsselt werden. Der zu diesem Zweck beim Sender benötigte öffentliche Empfängerschlüssel KAp kann diesem vom Empfänger über einen beliebigen unsicheren Kanal übermittelt werden. Natürlich könnte man die Nachricht auch direkt mit dem öffentlichen Empfängerschlüssel KAp

verschlüsseln, jedoch ist die erreichbare Performance der für eine asymmetrische Chiffre verfügbare Hardware und Software signifikant geringer als im Falle einer symmetrischen Chiffre, so daß bei großen Nachrichtenlängen und zur Erzielung einer hohen Verarbeitungsgeschwindigkeit die asymmetrische und symmetrische Chiffre meist in der in Fig. 3 gezeigten Kombination, nämlich einem Hybridverfahren, eingesetzt wird. In Fig. 4 wird durch die Verschlüsselung eines geheimen Parameters JV variabler Länge, zum Beispiel n · 180 Bit, mit einem symmetrischen Schlüssel KS, zum Beispiel 128 Bit, eine sehr lange (Pseudo)-Zufallszahl erzeugt, die als Vernam-Schlüssel KV schließlich die zu schützende Nachricht verschlüsselt. Für die Übermittlung des Ver- bzw. Entschlüsselungs-Schlüssels an den Empfänger braucht hier der Kurier jedoch nicht den Vernam-Schlüssel KV zu transportieren, sondern lediglich den Schlüssel KS und den Parameter IV, aus denen der Vernam-Schlüssel KV leicht auf Empfängerseite nachgebildet werden kann, da hier die gleiche Konfiguration wie auf der Senderseite vorhanden ist. In Fig. 5 ist die Verschlüsselung mit kombinierten asymmetrischen, symmetrischen und Vernam Chiffre gezeigt, wie in Fig. 4. Nach Fig. 5 wird im Gegensatz zur Fig. 4, die einen Kurier zum Austausch der geheimen Schlüsselinformationen benötigt, analog zu Fig. 3 hierfür eine asymmetrische Chiffre verwendet. Auf der Senderseite wird der öffentliche Empfängerschlüssel KAp eingespeist und auf der Empfängerseite der asymmetrische Senderschlüssel KAs.

Der Vorteil dieser Verfahrensweise wird in den Figuren 7 und 8 offenbart. In der jeweils oberen Bildhälfte der Fig. 6 und 7 sind daher je zwei typische Endgerätekonfigurationen dargestellt. Die grau unterlegten Elemente stellen die externe Kryptohardware, bestehend entweder aus einer Chipkarte oder aus einem Multifunktionalen PC Interface Adapter bzw. PCMCIA-Modul

mit eingebauter spezieller Kryptohardware oder einer eingebauten speziellen Chipkarte dar. Der Verschlüssler wird hingegen als herkömmlicher PC, mit Software oder einem anderen Endgerät realisiert, der jedoch außer der sehr einfachen Vernam Chiffre, wie zum Beispiel EXOR, welche sich auch für die breitbandigen Anwendungen in Software realisieren läßt, keine weitere Kryptotechnik benötigt. In beiden Figuren 6 und 7 ist gezeigt, daß die externen Kryptomodule alle komplexen Kryptofunktionen aufnehmen können, den Vernam-Schlüssel KV sozusagen als Vorrat erzeugen und in einem geeigneten Zwischenspeicher, dem KV Speicher ablegen, bis er vom Verschlüsselungsprozeß durch die logischen Operationen V nach und nach verbraucht wird. Dabei kann der KV Speicher entweder im Personal Computer bzw. Endgerät oder auch im Kryptomodul in Form einer Chipkarte oder eines PCMCIA Moduls eingebaut sein. Der Vorteil der Vorrichtungen nach den Figuren 6 und 7 besteht darin, daß der Verschlüssler immer mit der gleichen Vernam Chiffre arbeiten kann, auch wenn die externen Krypto- bzw. PCMCIA-Module unterschiedlich symmetrische und asymmetrische Chiffre verwenden. Die Vernam Chiffre ist auch für hohe Durchsatzraten in Software realisierbar, so daß alle Verschlüssler ohne aufwendige Kryptohardware auskommen und massenhaft und kostengünstig hergestellt werden können. Die externen Kryptomodule bleiben ebenfalls kostengünstig, da der auf Vorrat produzierte Vernam-Schlüssel auch von einer niedrig-performanten, das heißt langsamen Chipkarte, zum Beispiel auf Vorrat für den KV Speicher erzeugt werden kann, ohne den davon entkoppelt arbeitenden eigentlichen, breitbandigen Verschlüsselungsprozeß zu verlangsamen.

Die Verschlüssler werden aufgrund des beschriebenen Verfahrens von den Problemen teurer, hochperformanter und untereinander inkompatibler Kryptohardware befreit. Die Vernam Chiffre ist hingegen sehr einfach und kostengünstig

in Software zu implementieren. Alle komplexen Kryptofunktionen liegen außerhalb des Verschlüsslers. Der große Vorteil besteht auch noch darin, daß sie modular austauschbar sind und sich in den vorgeschlagenen preiswerten und langsamen, externen Kryptomodulen, zum Beispiel einer Chipkarte oder einer PCMCIA-Karte realisieren lassen. Die verwendeten Verfahren werden bei der Abstimmung zwischen Sender und Empfänger, zum Beispiel auf dem Übermittlungsweg ausgehandelt bzw. signalisiert.

Das Verfahren zur kostengünstigen Implementierung auch von hochperformanten Verschlüsselungsfunktionen in einem Verschlüssler, der lediglich aus einer PC Software oder einem beliebigen anderen Endgerät, Informationssystem mit integrierter Vernam Chiffre bestehen kann, die für den eigentlichen Verschlüsselungsprozeß nicht durch eine aufwendige Kryptohardware unterstützt werden muß, zeichnet sich dadurch aus, daß mittels eines geheimen Schlüssels KS mit einer definierten Schlüssellänge und mit Hilfe eines variablen Parameters mit einer bestimmten Bitlänge über eine beliebige symmetrische Chiffre S ein Vernam-Schlüssel KV mit der Länge der zu verschlüsselnden Nachricht erzeugt wird, welcher seinerseits über die Vernam Chiffre die zu schützende Nachricht verschlüsselt, wobei der geheime Schlüssel KS und der Parameter IV entweder über einen vom Nachrichtenübermittlungsweg getrennten, sicheren Kanal oder direkt auf dem Nachrichtenübermittlungsweg, zum Beispiel gesichert durch ein asymmetrisches Verfahren A vom Sender zum Empfänger übermittelt werden, wobei letzterer mit dem oben beschriebenen Verfahren den Vernam-Schlüssel KV regeneriert, um die empfangene Nachricht damit entschlüsseln zu können. Die symmetrische, gegebenenfalls auch die asymmetrische Chiffre und gegebenenfalls auch der Speicher für den Vernam-Schlüssel, nämlich der KV Speicher sind in einem vom Verschlüssler getrennten externen Kryptomodul, zum Beispiel in Form einer Chipkarte oder

eines PCMCIA-Moduls oder ähnlichem untergebracht und im Verschlüssler verbleiben lediglich die Vernam Chiffre und gegebenenfalls der Speicher KV für den Vernam-Schlüssel.

Liste der Bezugszeichen

KV	Vernam-Schlüssel
V	logische Operation, zum Beispiel EXOR
KS	geheimer symmetrischer Schlüssel
S	symmetrischer Chiffre, zum Beispiel IDEA
KAp	Empfänger-Schlüssel (asymmetrisch)
KAs	Sender-Schlüssel (asymmetrisch)
A	asymmetrischer Chiffre
IV	geheimer variabler Parameter
PCMCIA	Multifunktionaler PC Interface Adapter
PC-SW	PC Software

P A T E N T A N S P R Ü C H E

1. Verfahren zur vereinfachten Implementierung von Verschlüsselungsverfahren, insbesondere der Vernam Chiffre, wobei der Verschlüsselungsprozeß eine sehr einfache mathematische Operation, zum Beispiel EXOR, sein kann, dadurch gekennzeichnet,

   daß mittels eines geheimen Schlüssels (KS) mit einer definierten Schlüssellänge (x Bit) und mit Hilfe eines gegebenenfalls variablen Parameters (IV) mit einer Länge von n · x Bit über eine beliebige symmetrische Chiffre (S) ein Vernam-Schlüssel (KV) mit der Länge der zu verschlüsselnden Nachricht erzeugt wird,

   daß der Vernam-Schlüssel (KV) über logische Operationen der Vernam Chiffre (V) die zu schützende Nachricht verschlüsselt,

   daß der geheime Schlüssel (KS) und der Parameter (IV) über einen vom Nachrichtenübermittlungsweg getrennten, sicheren Kanal oder direkt auf dem Nachrichtenübermittlungsweg, gesichert durch ein asymmetrisches Verfahren (A) oder dergleichen, vom Sender zum Empfänger übermittelt werden, und

   daß der Empfänger den Vernam-Schlüssel (KV) regeneriert und damit die empfangene Nachricht entschlüsselt.

2. Verfahren nach Patentanspruch 1, dadurch gekennzeichnet,

   daß die symmetrische Chiffre und der Speicher für den Vernam-Schlüssel (KV) in einem vom Verschlüssler getrennten Kryptomodul in Form einer Chipkarte, eines

Multifunkionalen PC Interface Adapters bzw. -Moduls (PCMCIA) eingebracht werden und

daß im Verschlüssler nur die Vernam Chiffre Operationen durchgeführt werden.

3. Verfahren nach Patentanspruch 1, dadurch gekennzeichnet,

daß die asymmetrische Chiffre und der Speicher für den Vernam-Schlüssel (KV) in einem vom Verschlüssler getrennten externen Kryptomodul realisiert werden und

daß im Verschlüssler die Vernam Chiffre die Verschlüsslungsoperationen steuert.

4. Verfahren nach einem der Patentansprüche 1 bis 3, dadurch gekennzeichnet,

daß im Verschlüssler der Vernam-Schlüssel (KV) abgespeichert wird.

5. Vorrichtung zur Durchführung der Verfahren nach einem der Patentansprüche 1 bis 4, dadurch gekennzeichnet,

daß die Kryptohardware aus einer Chipkarte oder einem Multifunktionellen PC Interface Adapter (PCMCIA Modul) oder dergleichen mit eingebauter spezieller Kryptohardware besteht und

daß der Verschlüssler aus einem herkömmlichen Personalcomputer oder dergleichen, Software oder einem anderen Endgerät besteht, der eine sehr einfache Vernam Chiffre für breitbandige Anwendungen in Software realisiert, enthält.

6. Vorrichtung nach einem der Verfahren nach den Patentansprüchen 1 bis 4, dadurch gekennzeichnet,

daß die Kryptohardware als externes Kryptomodul ausgebildet ist und einen Zwischenspeicher zur Vorratsspeicherung des Vernam-Schlüssels (KV) aufweist.

7. Vorrichtung nach einem der Patentansprüche 6 bzw. 7, dadurch gekennzeichnet,

daß der Speicher zum Speichern des Vernam-Schlüssels (KV) entweder im Personalcomputer (PC) oder in einem sonstigen Endgerät angeordnet ist.

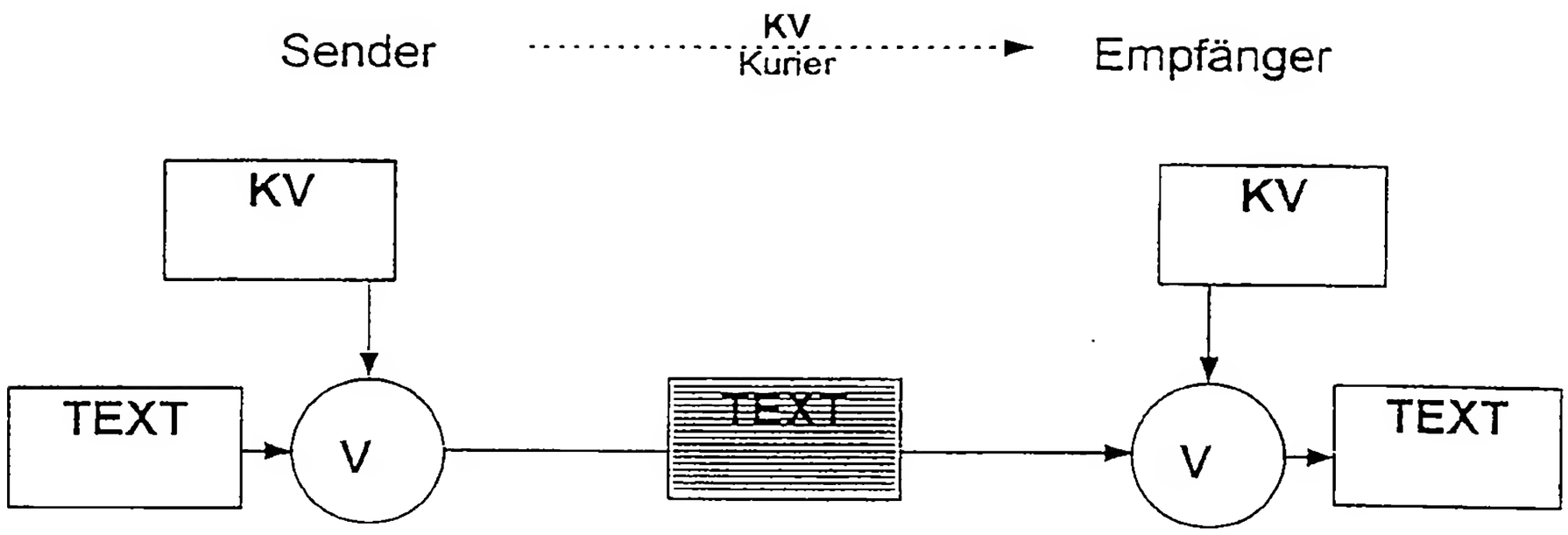

Sender
KV
Kurier
Empfänger
KV
KV
TEXT
V
TEXT
V
TEXT

FIG. 1

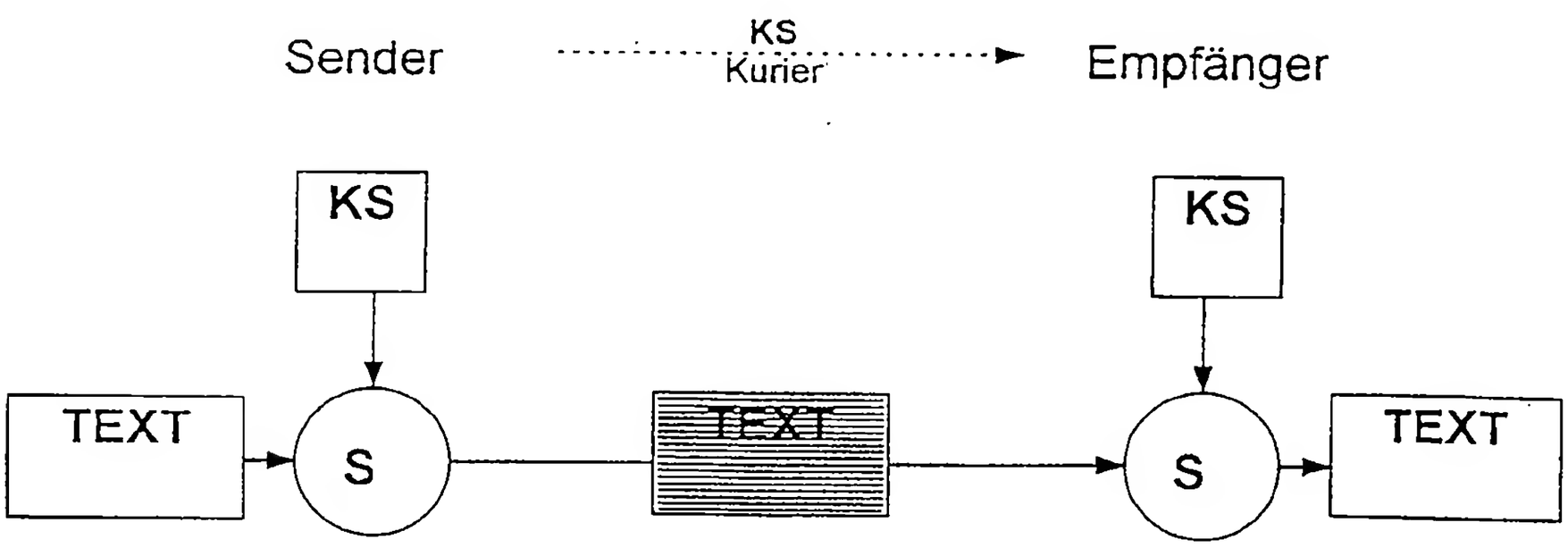

Sender
KS
Kurier
Empfänger
KS
KS
TEXT
S
TEXT
S
TEXT

FIG. 2

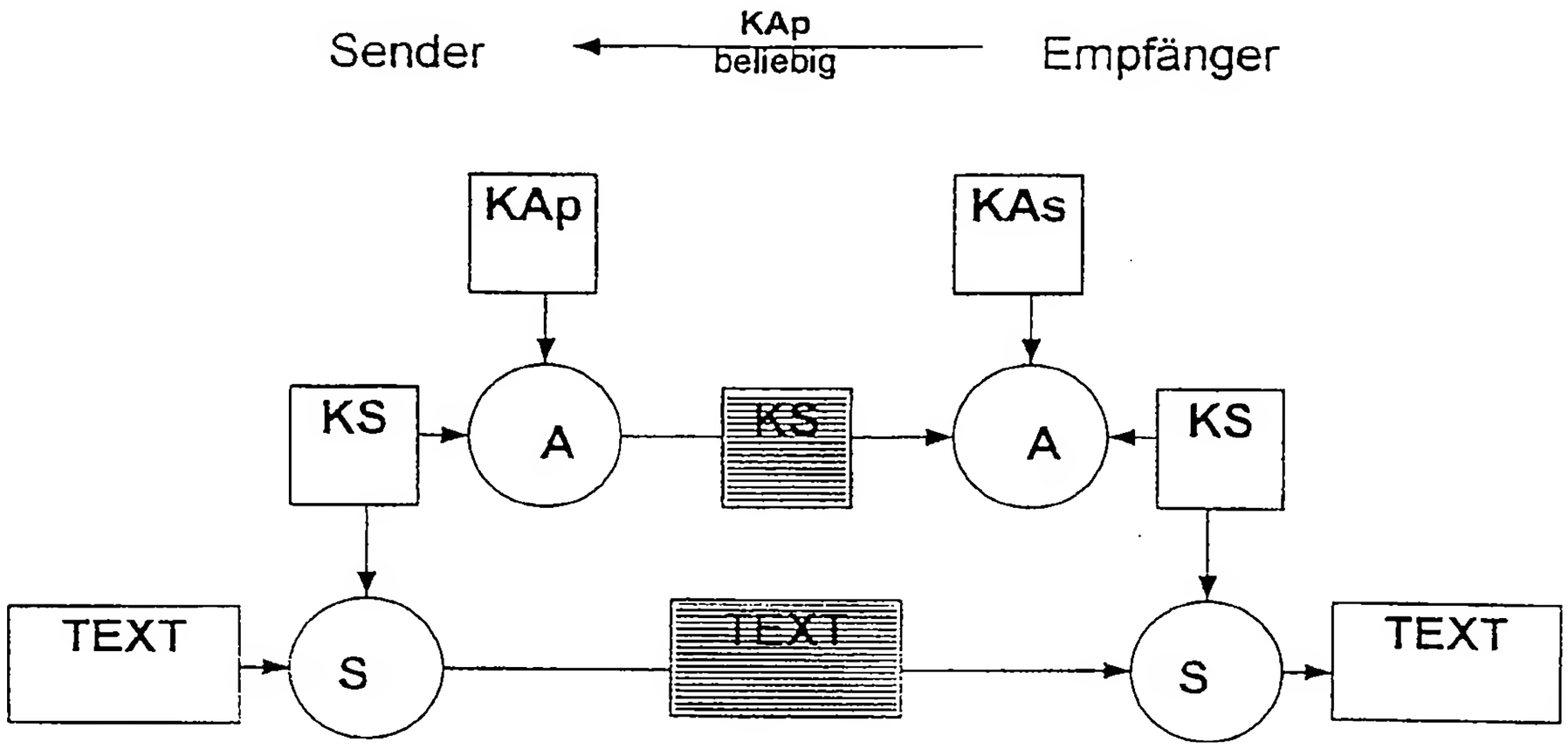

Sender
KAp
beliebig
Empfänger
KAp
KAs
KS
A
KS
A
KS
TEXT
S
TEXT
S
TEXT

FIG. 3

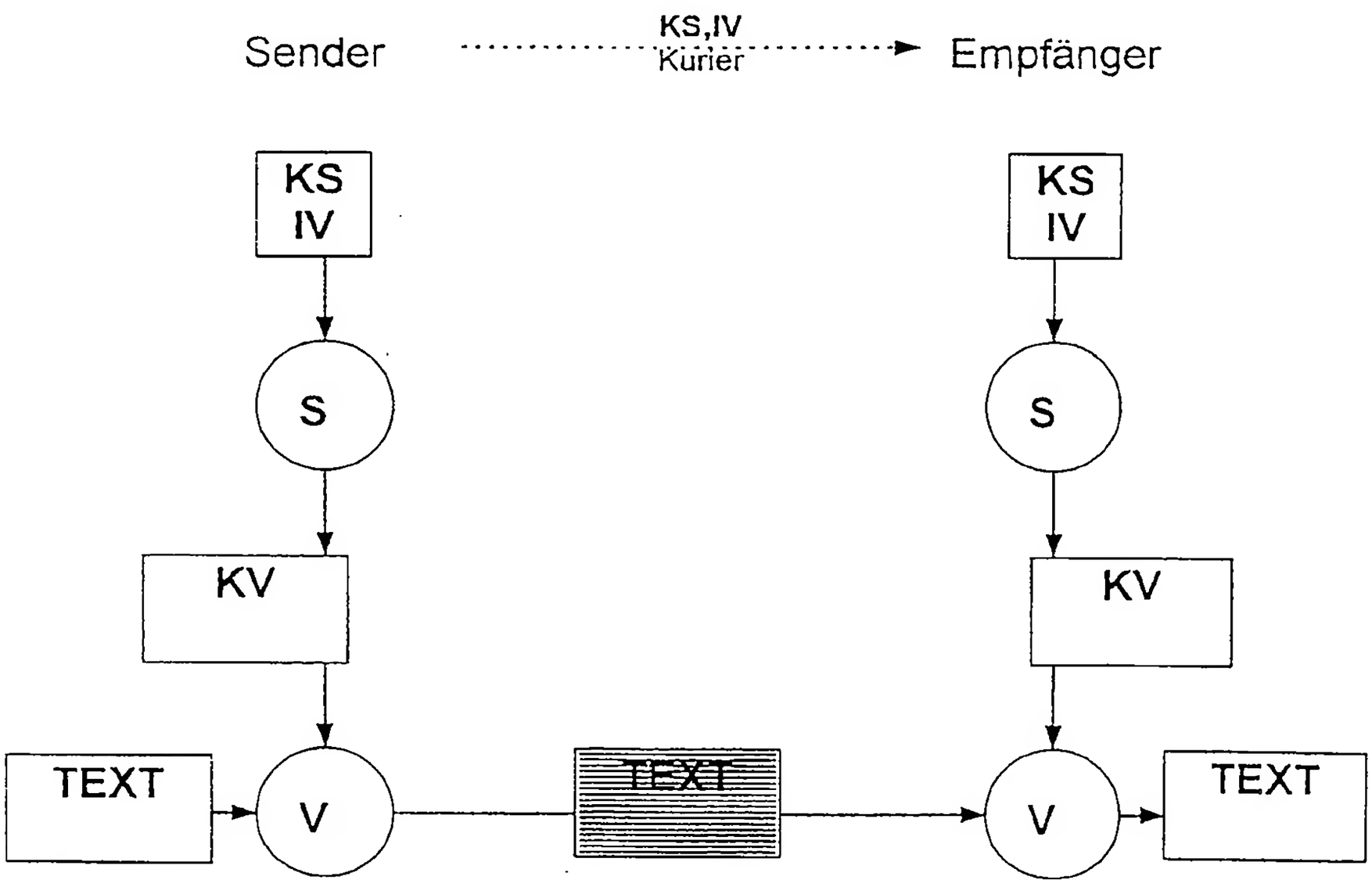

Sender
KS,IV
Kurier
Empfänger
KS
IV
KS
IV
S
S
KV
KV
TEXT
V
TEXT
V
TEXT

FIG. 4

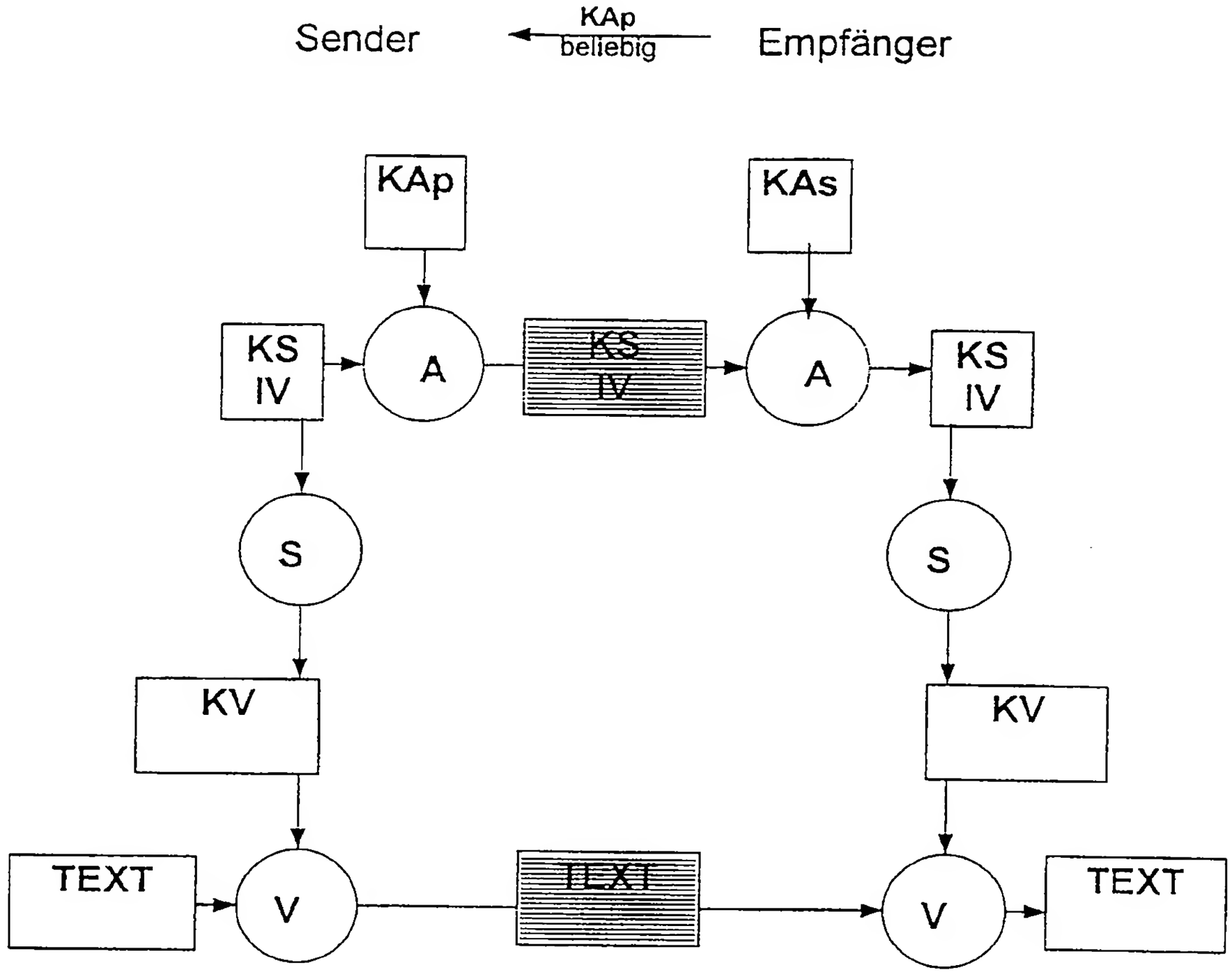

Sender
KAp
beliebig
Empfänger
KAp
KAs
KS
IV
A
KS
IV
A
KS
IV
S
S
KV
KV
TEXT
V
TLXT
V
TEXT

FIG. 5

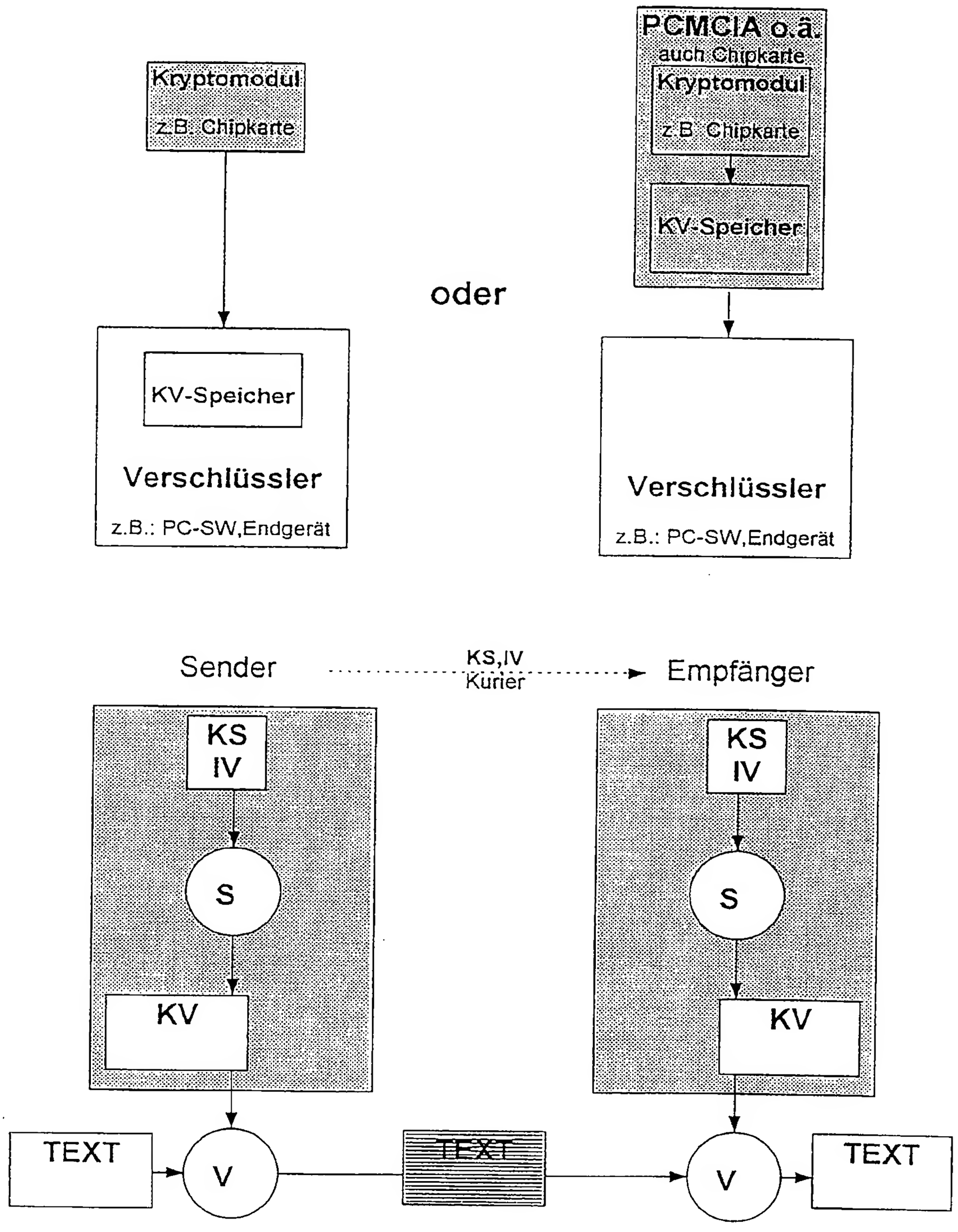

Kryptomodul
z.B. Chipkarte
KV-Speicher
Verschlüssler
z.B.: PC-SW,Endgerät
oder
PCMCIA o.ä.
auch Chipkarte
Kryptomodul
z.B. Chipkarte
KV-Speicher
Verschlüssler
z.B.: PC-SW,Endgerät
Sender
KS,IV
Kurier
Empfänger
KS
IV
S
KV
KS
IV
S
KV
TEXT
V
TEXT
V
TEXT

FIG. 6

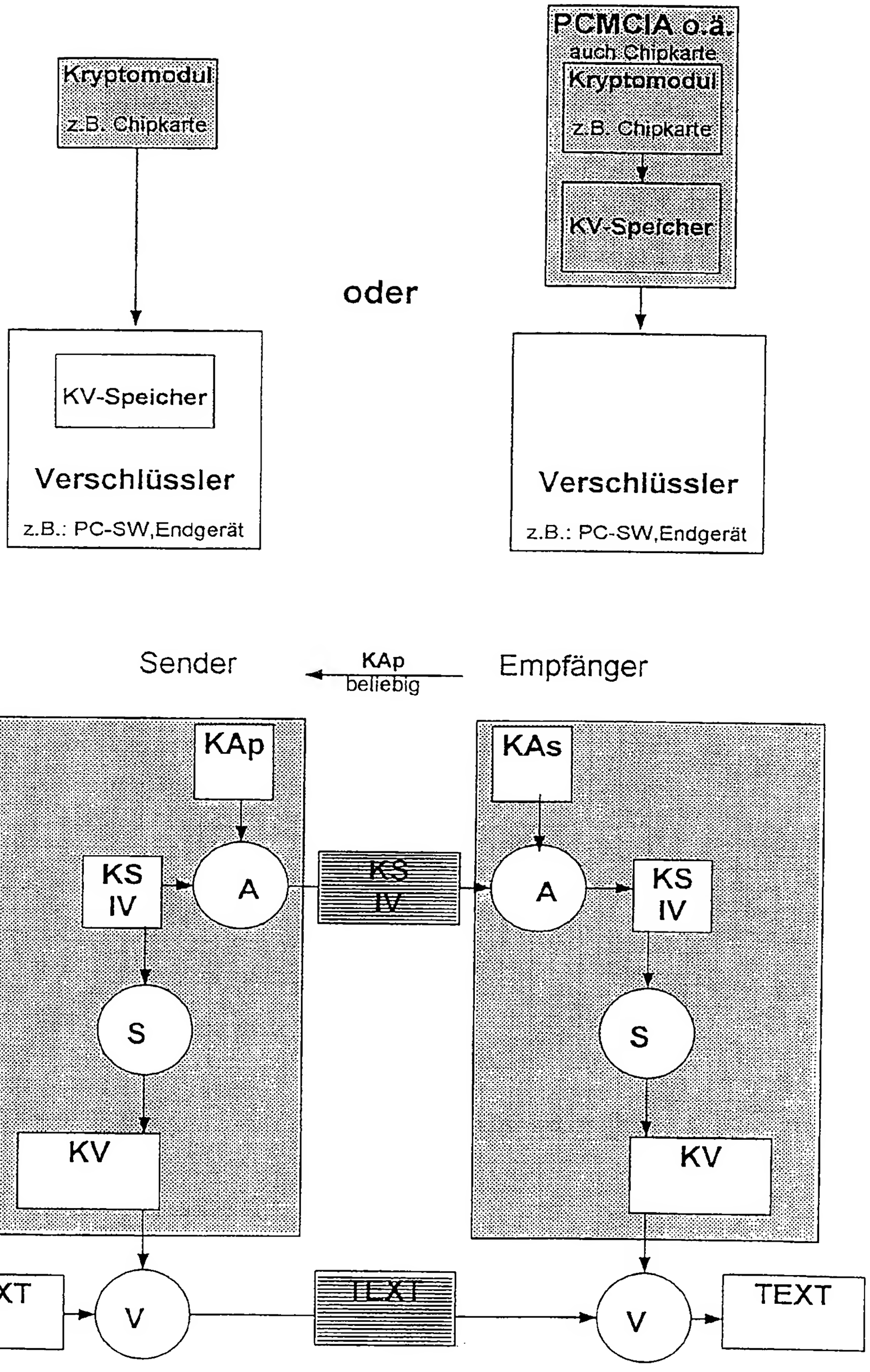

Kryptomodul
z.B. Chipkarte
KV-Speicher
Verschlüssler
z.B.: PC-SW,Endgerät
oder
PCMCIA o.ä.
auch Chipkarte
Kryptomodul
z.B. Chipkarte
KV-Speicher
Verschlüssler
z.B.: PC-SW,Endgerät
Sender
KAp
beliebig
Empfänger
KAp
KS
IV
A
S
KV
KS
IV
KAs
A
KS
IV
S
KV
TEXT
V
TEXT
V
TEXT

FIG. 7

INTERNATIONAL SEARCH REPORT

	I ıational Application No PCT/EP 98/01391

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/18 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FEY P: "VERSCHLUESSELUNG VON SPRACHE UND DATEN" NACHRICHTENTECHNIK ELEKTRONIK, vol. 40, no. 10, 1 January 1990, pages 376-377, XP000176445 BERLIN (DE)	1
Y	see page 376, right-hand column, last paragraph - page 377, right-hand column, last line	2

A	DE 27 06 421 B (LICENTIA) 29 June 1978 see column 3, line 61 - column 5, line 28	1

Y	EP 0 616 429 A (SIEMENS) 21 September 1994	2
A	see column 1, line 28 - line 50 see column 3, line 38 - column 4, line 11	5,6

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 September 1998	08/09/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

	International Application No PCT/EP 98/01391

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4 974 193 A (BEUTELSPACHER ETAL.) 27 November 1990 see column 2, line 49 - column 3, line 41	2
A	US 5 513 261 A (MAHER) 30 April 1996 see column 2, line 27 - line 62 see column 3, line 16 - line 21	2

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 98/01391

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 2706421 B	29-06-1978	AT 376344 B	12-11-1984
		AT 87678 A	15-03-1984
		CH 639229 A	31-10-1983
		FR 2381423 A	15-09-1978
		GB 1598415 A	23-09-1981
		NL 7801619 A	18-08-1978
		US 4211891 A	08-07-1980
EP 616429 A	21-09-1994	JP 6244684 A	02-09-1994
US 4974193 A	27-11-1990	DE 3706955 A	15-09-1988
		DE 3889481 D	16-06-1994
		EP 0281057 A	07-09-1988
		ES 2051780 T	01-07-1994
		JP 63228353 A	22-09-1988
US 5513261 A	30-04-1996	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 98/01391

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/18 G07F7/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	FEY P: "VERSCHLUESSELUNG VON SPRACHE UND DATEN" NACHRICHTENTECHNIK ELEKTRONIK, Bd. 40, Nr. 10, 1. Januar 1990, Seiten 376-377, XP000176445 BERLIN (DE)	1
Y	siehe Seite 376, rechte Spalte, letzter Absatz - Seite 377, rechte Spalte, letzte Zeile	2

A	DE 27 06 421 B (LICENTIA) 29. Juni 1978 siehe Spalte 3, Zeile 61 - Spalte 5, Zeile 28	1

	-/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
2. September 1998	08/09/1998
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	**Bevollmächtigter Bediensteter** Holper, G

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

ii ationales Aktenzeichen
PCT/EP 98/01391

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	EP 0 616 429 A (SIEMENS) 21. September 1994	2
A	siehe Spalte 1, Zeile 28 - Zeile 50 siehe Spalte 3, Zeile 38 - Spalte 4, Zeile 11	5,6

Y	US 4 974 193 A (BEUTELSPACHER ETAL.) 27. November 1990 siehe Spalte 2, Zeile 49 - Spalte 3, Zeile 41	2

A	US 5 513 261 A (MAHER) 30. April 1996 siehe Spalte 2, Zeile 27 - Zeile 62 siehe Spalte 3, Zeile 16 - Zeile 21	2

1